AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (currently amended) A method for establishing a secure network connection between a client ~~platform~~ web browser and a service, said client having resources including a web browser ~~having~~ with a virtual machine, ~~and knowing and trusting~~said web browser having access to a first ~~public~~ key, said client web browser and virtual machine being of the type that downloads and executes applets while protecting against at least some of said client resources from being updated based on said applet execution, said method comprising:

establishing an insecure network connection with said client web browser;

downloading, over said insecure connection, at least one digitally signed applet to the client ~~platform~~web browser, said at least one applet ~~comprising~~ including: (a) a second key, (b) code ~~that is~~ executable on the client ~~platform~~ virtual machine to cause the client ~~platform~~ to store a second ~~public~~ key, and (c) code executable on the client virtual machine to use the stored second key establish a secure network connection with said service; ~~that allows authentication between the client platform and the service~~;

before the client ~~platform~~ virtual machine executes the digitally signed applet, verifying the digitally signed applet at the client ~~platform~~ using the first ~~public~~ key ~~the client platform already knows and trusts~~;

executing the downloaded applet code with the client ~~platform~~ virtual machine, thereby causing the client ~~platform~~ to store a second ~~public~~ key corresponding to the service; and

further executing said at least one applet to cause said at least one applet to use ~~using~~ the stored second ~~public~~ key to authenticate the service and establish the secure network connection with the service.

2. (currently amended) The method of claim 1 wherein the applet includes a second ~~public~~ key payload and further includes first program code that controls the client ~~platform~~ to store the second ~~public~~ key to a non-volatile memory.

3. (previously presented) The method of claim 2 wherein the non-volatile memory comprises a disk.

4. (currently amended) The method of claim 2 wherein the applet further includes second program code that controls the client ~~platform~~ to use the stored second ~~public~~ key to verify a signature subsequently provided by the server.

5. (currently amended) The method of claim 1 wherein the applet further includes program code that controls the client ~~platform~~ to use the stored second ~~public~~ key to verify a signature subsequently provided by the server.

6. (currently amended) The method of claim 1 wherein the executing step includes controlling the client ~~platform~~ virtual machine to store, at the client, a second ~~public~~ key in the form of a digital certificate corresponding to the server, and the ~~using~~ further executing step comprises receiving a digital signature from the server, and authenticating

the received digital signature under control of the executing applet through use of the stored digital certificate corresponding to the server.

7. (currently amended) The method of claim 1 wherein the ~~using~~ further executing step includes having the executing applet invoke a further applet to establish a secure connection.

8. (currently amended) The method of claim 1 wherein the applet comprises a signed Archive containing a digital certificate corresponding to the server, and a program fragment that stores the digital certificate in a predetermined location on the client ~~platform~~ that permits the client ~~platform~~ to later retrieve the stored digital certificate.

9. (currently amended) A client ~~platform~~ web browser for establishing a secure network connection with-a service over a network, said client ~~platform~~ ~~having~~ web browser including a virtual machine ~~and knowing and trusting a first public key~~, said client web browser and virtual machine being of the type that download and execute applets while protecting against at least some of said client resources from being updated by said applet execution, said client ~~platform~~ comprising:

an applet receiver that receives ~~a~~ at least one digitally signed applet from the service over ~~the~~ an insecure network connection, said at least one applet including: (a) a key, (b) code executable on the client virtual machine to cause the client to store the key, and (c) code executable on the client virtual machine to establish a secure network connection with said service, said applet being ~~executable~~ executed by the client ~~platform~~ virtual machine to cause the client ~~platform~~ to store ~~a second~~the ~~public~~ key delivered with the applet, the stored key allowing ~~that allows~~ authentication between the client ~~platform~~ and the service;

wherein the client ~~platform~~ ~~virtual machine~~web browser includes an applet verifier that, before executing the applet, verifies the digitally signed applet using a ~~first public key the client platform already knows and trusts~~key different from the key delivered with the applet;

wherein the client ~~platform~~ virtual machine further includes an applet executor that executes the applet, thereby controlling the client ~~platform~~ to store ~~a second public~~the key delivered with the applet, said delivered key corresponding to the server, and uses the stored delivered ~~second public~~ key to authenticate the ~~service~~ server and establish ~~the~~ a secure network connection between the client and the server.

10. (currently amended) A method for establishing a secure network connection with a client web browser, said client ~~platform~~ ~~virtual machine~~ web browser including a virtual machine, said client web browser and virtual machine being of the type that download and execute applets while protecting at least some of client resources from being affected by said applet execution, the method comprising:

downloading, over an insecure network connection, ~~an~~ at least one executable applet to the client ~~platform~~ virtual machine, said at least one applet including: (a) a further key corresponding to the server, (b) code executable on the client virtual machine to cause the client to store the further key corresponding to the server, and (c) code executable on the client virtual machine to establish a secure network connection with said server, the digitally signed applet being digitally signed such that the client ~~platform~~ virtual machine can verify the digitally signed applet using a first ~~public~~ key the client ~~platform~~ ~~already knows and trusts~~possesses before said downloading, the at least one digitally signed applet including ~~a~~the ~~second public~~ further key and code executable by the client ~~platform~~ virtual machine that controls the client ~~platform~~ virtual machine to store the ~~second public key on the client platform~~further key;

sending a digital credential to the client, said digital credential being verifiable by the client ~~platform~~ applet using the stored ~~second public~~further key delivered with the at least one applet; and

establishing a secure network communication with the executing client applet based on said digital credential as verified by the client applet.

11. (currently amended) The method of claim 10 wherein the applet code controls the client ~~platform~~ to store the ~~second public~~further key to a non-volatile memory.

12. (previously presented) The method of claim 11 wherein the non-volatile memory comprises a disk.

13. (currently amended) The method of claim 10 wherein the applet further includes further code that controls the client ~~platform~~ to use the stored ~~second public~~further key to verify the digital credential.

14. (currently amended) The method of claim 10 further including sending a further applet to the client ~~platform~~ in response to an invocation of the further applet by the ~~first-mentioned~~at least one applet.

15. (currently amended) The method of claim 10 wherein the applet comprises a signed Archive containing a digital certificate, and a program fragment that stores the digital certificate in a predetermined location on the client ~~platform~~ that permits the client ~~platform~~ to later retrieve the stored digital certificate.

16. (currently amended) A server for establishing a secure network connection with a client web browser over a network, said client having resources including the web browser and a virtual machine ~~and knowing and trusting a first public key~~, said client web browser and virtual machine being of the type that download and execute applets while protecting at least some of said client resources from being affected by said applet execution, said server comprising:

an applet transmitter that transmits ~~a~~ at least one digitally signed applet to the client over ~~the~~ an insecure network connection, the at least one applet being digitally signed using ~~the~~ a first ~~public~~ key the client ~~already knows and trusts~~possesses independently of the applet, said at least one applet including: (a) a second key corresponding to the server, (b) code executable on the client virtual machine to cause the client to store the second key, and (c) code executable on the client virtual machine to establish a secure network connection with said server, the applet being executable by the client virtual machine to control the client to store the ~~a~~ second ~~public~~ key corresponding to the server; ~~and~~

a digital credential transmitter that transmits a digital credential to the client executing the applet, the digital credential being authenticatable by the client using the second ~~public~~ key; and

a secure network connector that establishes a secure network connection with the client under control of the executing applet and based at least in part on the digital credential being authenticated by the second key delivered over the insecure network connection..

17. (currently amended) A method for establishing a secure network connection between a server and a web browser having access to a first~~, trusted public~~ key and also having a virtual machine, said web browser and virtual machine downloading and executing applets while protecting resources from being updated by said applet execution, said method comprising:

downloading, to the browser over an insecure network connection, ~~a~~ at least one digitally signed applet ~~including executable code from the server to the browser~~, the applet including: (a) a second ~~public~~ key associated with the server, (b) code executable on the client virtual machine to cause the client to store the second key, and (c) code executable on the client virtual machine to establish a secure network connection with said server;

verifying the digitally signed applet at the browser using the first ~~public~~ key;

executing the applet with the virtual machine to cause the client to store the second ~~public~~ key ~~into a certificate store associated with the browser in response to the verifying step~~; ~~and~~

using the stored second ~~public~~ key to authenticate ~~the~~ a further credential delivered by the server; and

based on said authentication of said further credential, establishing, under control of the executing applet, a secure network connection between the web browser and the server.

18. (previously presented) A method as in claim 17 wherein the applet comprises an archive.